Checking safety in Exactly-once - a library for stronger message processing guarantees

Tomek Masternak, Szymon Pobiega
Particular Software

Exactly-once is a software library that provides stronger processing guarantees in systems built on top of at-least-once message delivery infrastructure. It assumes that system consists of message processing handlers each managing a single, dedicated transactional resource, that communicate by exchanging messages. The library ensures that observable side-effects produced by a handler are equivalent to one of possible sequential message processing. It does so by providing consistency between input message, transactional resource modification, and output messages under possible delivery anomalies i.e. duplication and re-ordering as well as infrastructure failures.

The library uses simplified atomic commit protocol. The protocol involves a resource with optimistic concurrency support acting as the voter, and an message queues always able to commit successfully. The library manages its operational state without atomic guarantees between the state and transactional resource managed by the handler - current implementation supports handlers with business data stored in one CosmosDB partition and the operational state in another one.

A system using the library has been modelled in PlusCal and checked for safety. The safety formula validates that in a multi-handler environment with message processing failures and delivery anomalies, for each input message there is at most one transactional resource change and at most one output message.